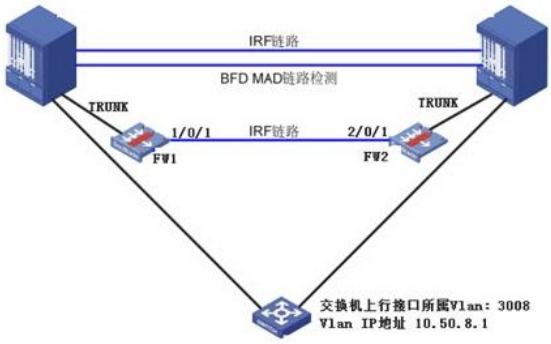
SecBlade IV防火墙插卡配置跨Vlan二层转发数据不通问题解决方法

二层转发 刘嘉炜 2019-05-16 发表

组网及说明



.

问题描述

现场两台S75E交换机、两块SecBlade IV插卡堆叠部署，配置跨Vlan二层转发功能后发现数据不通。

过程分析

防火墙涉及配置：

1、排查安全策略及安全域，发现没有问题。

#

security-zone intra-zone default permit

#

session synchronization enable

#

zone-pair security source Any destination Any

packet-filter 3000

#

security-zone name Trust

import vlan 8 3008

2、查看冗余组配置及端口聚合状态均正常

[Intra_fw01]display redundancy group

Redundancy group red (ID 1):

Node ID	Slot	Priority	Status	Track weight
1	Slot1	100	Primary	255
2	Slot2	50	Secondary	255

Node 1:

Node member	Physical status
XGE1/0/1	UP
XGE1/0/2	UP
XGE1/0/3	UP

Track info:

Track	Status	Reduced weight	Interface
1	Positive	255	XGE1/0/1
2	Positive	255	XGE1/0/2
3	Positive	255	XGE1/0/3

端口聚合选中状态也正常：

[Intra_fw01]display link-aggregation verbose

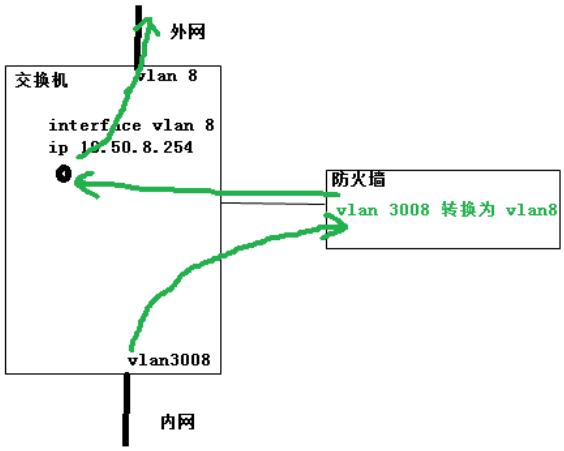
Port	Status	Priority	Oper-Key
XGE1/0/1	S	1	2
XGE1/0/2	S	1	2
XGE1/0/3	S	1	2
XGE2/0/1	U	2	2
XGE2/0/2	U	2	2
XGE2/0/3	U	2	2

查看跨Vlan 二层转发配置:

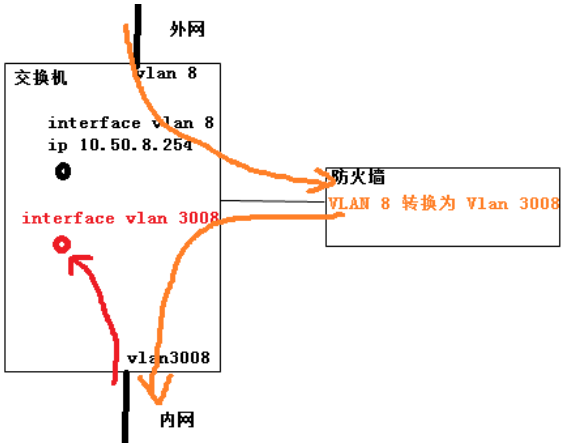
#
bridge 1 inter-vlan
add vlan 8 3008
#
查看桥组有学习到的MAC地址，发现学习的表项均是正常的。对于二层报文来说表象正常说明是可以通信的，但是现场数据还是不通。
[Intra_fw01]display bridge mac-address
MAC Address BRIDGE ID State VLAN ID Port Aging
04d7-a595-be01（核心交换机VLAN 8 MAC） 1 Learned 8 BAGG1 Y
7485-c4ba-820c（测试交换机Vlan3008 MAC）1 Learned 3008 BAGG1 Y
继续排查发现核心交换机有10.50.8.1设备的ARP，但是在测试交换机上却没有核心交换机的ARP和MAC地址表象，这点很奇怪。
核心交换机：
[核心交换机]dis arp
Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid
IP address MAC address VLAN/VSI Interface Aging Type
10.50.8.1 7485-c4ba-820c 8 BAGG20 971 D
测试交换机：
<测试交换机>dis arp
Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid
IP address MAC address VLAN/VSI Interface Aging Type

交换机配置排查：
核心交换机聚合状态正常：
[core_sw01]display link-aggregation verbose
Port Status Priority Oper-Key
XGE1/6/0/1(R) S 1 1
XGE1/6/0/2 S 1 1
XGE1/6/0/3 S 1 1
XGE2/6/0/1 U 32768 1
XGE2/6/0/2 U 32768 1
XGE2/6/0/3 U 32768 1
在查看核心交换机的配置后发现核心交换机配置了vlan 3008的虚接口?
[core_sw01]dis ip in br
*down: administratively down
(s): spoofing (l): loopback
Interface Physical Protocol IP address VPN instance Description
MGE1/0/0/0 down down -- -- --
MGE1/0/0/1 down down -- -- --
MGE1/0/0/2 down down -- -- --
MGE1/0/0/3 down down -- -- --
Vlan8 up up 10.50.8.254 -- Manage_TO_...
Vlan10 up up 10.50.10.254 -- Test_TO_Ac...
Vlan21 up up 10.50.21.254 -- Office_TO_...
Vlan23 up up 10.50.23.254 -- Ops_TO_Acc...
Vlan25 up up 10.50.25.254 -- Internet_T...
Vlan26 up up 10.50.26.254 -- Connect_TO...
Vlan30 up up 10.50.30.254 -- Online_TO_...
Vlan40 up up 10.50.40.254 -- Bigdata_TO...
Vlan150 up up 10.150.10.254 -- ILO_TO_Acc...
Vlan3008 up up -- -- --

防火墙正常跨vlan二层报文转发流程：



防火墙异常跨vlan二层报文转发流程：



1、 如上图所示看到黄色为下行流量，下行流量转发是正常的，所以在交换机上可以看到测试交换机的arp信息。

2、 但是上行流量就出现了问题，如果核心交换机配置了三层接口，那么数据会直接上送交换机做三层转发，直接由CPU处理，CPU查表项直接丢弃报文。因此数据根本就不会上送到防火墙做跨vlan二层转发。

解决方法

删除核心交换机空闲的Vlan接口，让数据通过二层泛洪到防火墙接口做替换标签操作。

跨Vlan二层转发注意事项：

在配置跨Vlan二层转发时一定要注意在交换机上不能配置转换前VLAN的虚接口，如果配置会导致交换机认为报文需要做三层转发到CPU直接丢弃。